JOURNAL OF ALGEBRA **184,** 1143–1160 (1996)
ARTICLE NO. 0304

On Brauer's $k(B)$-Problem

Geoffrey R. Robinson

Department of Mathematics & Computer Science, University of Leicester, Leicester LE1 7RH, England

John G. Thompson*

Department of Mathematics, University of Florida, P.O. Box 118000, Gainesville, Florida 32611-8000

Communicated by Walter Feit

Received October 25, 1995

INTRODUCTION

A long-standing problem of R. Brauer is to prove that whenever B is a block with defect group D of a finite group, then $k(B)$, the number of ordinary irreducible characters in B, is at most $|D|$. In this paper, we provide an affirmative solution to the problem for blocks of p-solvable groups, for all but an explicit finite number of primes. This result has implications for the structure of blocks of general finite groups, in the light of other current conjectures.

By the results of Fong [1] and Nagao [9], Brauer's problem reduces in the p-solvable case to the "$k(GV)$-problem," which is to prove that whenever p is a prime, G is a finite p'-group, and V is faithful $GF(p)G$-module, then $k(GV)$, the number of conjugacy classes of the semi-direct product GV, is at most $|V|$. In fact, it suffices to consider the case that G acts irreducibly on V.

The $k(GV)$-problem has some interest in its own right, but it has so far proved to be extremely stubborn in its full generality. Partial results have

* Research of second author supported by the National Science Foundation under Grant DMS-9401399.

0021-8693/96 $18.00

been obtained by Gluck [2], Gow [3] and Knörr [5, 6], with Knörr providing the fundamental idea underpinning most attacks on the problem to date. The character theory of this paper is influenced to a large extent by the work of Gow and Knörr.

Our main result is:

THEOREM 1. *Let p be a prime with $p > 5^{30}$, B be a p-block with defect group D of a p-solvable finite group. Then $k(B) \leq |D|$.*

This relies on the solution (for primes $p > 5^{30}$) of the $k(GV)$-problem, which is provided by the following two results.

THEOREM 2. *Let p be a prime, G be a finite p'-group, V be a faithful irreducible $GF(p)G$-module. Suppose that there is a vector $v \in V$ such that $\mathrm{Res}^G_{C_G(v)}(V)$ has a faithful self-dual submodule. Then $k(GV) \leq |V|$.*

THEOREM 3. *Let p be a prime with $p > 5^{30}$, G be a finite p'-group, V be a faithful irreducible $GF(p)G$-module. Then there is a vector $v \in V$ such that $\mathrm{Res}^G_{C_G(v)}(V)$ has a faithful submodule which is a permutation module (so it is certainly self-dual).*

The proof of Theorem 2 is subsumed within the proof of a rather more technical, and somewhat stronger, Theorem 4, whose statement we defer for the moment. The proof of Theorem 3 relies ultimately on the classification of the finite simple groups, through a recent improvement by Liebeck [8] of a result of Hall, Liebeck, and Seitz [4]. If the bound 5^{30} appearing in Liebeck's theorem could be improved to some smaller integer N, then our bound in Theorems 1 and 3 could be improved to $\max(6815, N)$.

1. THE CHARACTER THEORY: NOTATION AND GENERAL REMARKS

We fix a prime p, a finite p'-group G, and a faithful irreducible $GF(p)G$-module V. We set $\omega = \exp(2\pi i/|G|)$, and let σ denote that element of $\mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ with $\omega^\sigma = \omega^p$. We let Φ denote the Brauer character of G afforded by V, and we fix an irreducible complex constituent χ of Φ. We let τ denote a generator of $\mathrm{Stab}_{\langle\sigma\rangle}(\chi)$. Notice that $\Phi = \sum_{\gamma \in \langle\sigma\rangle/\langle\tau\rangle} \chi^\gamma$.

Suppose that there is an irreducible $GF(p)G$-module W with $W \cong W^*$ and let W afford Brauer character ϕ. Then $\phi = \overline{\phi}$. Since ϕ is the sum of irreducible complex characters of G which are transitively permuted by $\langle\sigma\rangle$, we see that when μ is a complex irreducible constituent of ϕ, μ, and $\overline{\mu}$ are in the same $\langle\sigma\rangle$-orbit. If U is a $GF(p)G$-module with $U \cong U^*$ and U has an irreducible submodule W with $W \ncong W^*$, then U has a submodule isomorphic to W^*. In that case, the irreducible constituents of the Brauer character of W are transitively permuted by $\langle \sigma \rangle$, and if μ is one of them, then μ and $\overline{\mu}$ are in different $\langle \sigma \rangle$-orbits.

Since G is a p'-group, we can go somewhat further:

Let μ be a complex irreducible character of G, and suppose that there is some $\gamma \in \mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ such that μ and μ^γ are in different $\langle \sigma \rangle$-orbits. Then $\sum_\lambda \mu^\lambda$ is the Brauer character is an irreducible $GF(p)G$-module, U say (where λ runs through a transversal T to $\mathrm{Stab}_{\langle \sigma \rangle}(\mu)$ in $\langle \sigma \rangle$). Similarly, $\sum_{\lambda \in T} \mu^{\gamma^\lambda}$ is the Brauer character of another irreducible $GF(p)G$-module, which we label U^γ. Although U and U^γ are not isomorphic $GF(p)G$-modules, we still have $|C_U(g)| = |C_{U^\gamma}(g)|$ for all $g \in G$, a fact which we will exploit below.

We recall the well-known fact that induction of class functions yields a bijection between generalized characters of G and generalized characters of GV which vanish off p-regular elements. Furthermore, for any generalized character, θ, of G, we have $\mathrm{Ind}_G^{GV}(\theta)[g] = |C_V(g)|\theta(g)$ for all $g \in G$. A consequence of these facts which we will frequently use is that whenever ψ is a generalized character of GV which vanishes off p-regular elements, the class function, θ, of G with $\theta(g) = |C_V(g)|^{-1}\psi(g)$ for all $g \in G$ is a generalized character of G.

2. PROOFS OF THE CHARACTER-THEORETIC THEOREMS

The proof of Theorem 2 is included in the proof of the somewhat more technical:

THEOREM 4. *Let $G, V, \Phi, \chi, \sigma, \tau$ be as in Section* 1. *Suppose that $k(GV) > |V|$. Choose $v \in V$, and set $H = C_G(v)$. Let β be the sum of those irreducible constituents ϕ of $\mathrm{Res}_H^G(\chi)$ such that*:

(i) *The algebraic conjugates of ϕ which occur as irreducible constituents of $\mathrm{Res}_H^G(\chi)$ are transitively permuted by $\langle \tau \rangle$.*

(ii) $\mathrm{Stab}_{\langle \sigma \rangle}(\phi) \subseteq \langle \tau \rangle$.

(iii) $\mathrm{Res}_H^G(\chi)$ *contains ϕ with multiplicity* 1.

(iv) *The character $\overline{\phi}$ is in a different $\langle \sigma \rangle$-orbit from ϕ.*

Then $\mathrm{Res}_H^G(\chi) - \beta$ is not faithful.

Proof. Let $\psi = \mathrm{Res}_H^G(\Phi)$. We will prove that it is not possible to find irreducible constituents $\phi_1, \phi_2, \ldots, \phi_t$ of ψ such that:

(i) $\sum_{i=1}^t \phi_i$ is a faithful character of H.

(ii) No two of the ϕ_i are algebraically conjugate.

(iii) For each i, at least one of the following conditions is satisfied:

(a) ϕ_i occurs with multiplicity greater than one in ψ.

(b) An algebraic conjugate of ϕ_i in a different $\langle \sigma \rangle$-orbit from ϕ_i occurs as a constituent of ψ.

(c) $\overline{\phi}_i$ is in the same $\langle \sigma \rangle$-orbit as ϕ_i.

We first explain how Theorems 2 and 4 both follow, once we have established this. Suppose that $\mathrm{Res}^G_H(V)$ has a faithful submodule U for which $U \cong U^*$. Let μ be the Brauer character afforded by U. Whenever ϕ is an irreducible constituent of μ, $\overline{\phi}$ is also a constituent. If $\overline{\phi}$ is in the same $\langle \sigma \rangle$-orbit as ϕ, then ϕ satisfies condition (c) above. Otherwise, ϕ satisfies condition (b) above. In this case, then, we may take $\{\phi_i : 1 \leq i \leq t\}$ to be a set of irreducible constituents of μ which is maximal subject to the property that no two of the ϕ_i are algebraically conjugate, and we obtain a contradiction.

Suppose next that $\mathrm{Res}^G_H(\chi) - \beta_1$ is faithful, where β_1 is the sum of those irreducible constituents ϕ of $\mathrm{Res}^G_H(\chi)$ for which none of conditions (a), (b), (c) above hold. Then we can find $\{\phi_i : 1 \leq i \leq t\}$, a set of irreducible constituents of ψ, with the properties outlined above, a contradiction. Thus $\mathrm{Res}^G_H(\chi) - \beta_1$ is not faithful. Let ϕ be an irreducible constituent of β_1. Then ϕ certainly occurs with multiplicity one in $\mathrm{Res}^G_H(\chi)$. If there is some $\alpha \in \mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ such that ϕ^α is in a different $\langle \tau \rangle$-orbit from ϕ, but ϕ^α occurs with non-zero multiplicity in $\mathrm{Res}^G_H(\chi)$, then since condition (b) fails for ϕ, we have $\phi^\alpha = \phi^{\sigma^i}$ for some integer i. Then $\chi^{\sigma^i} \neq \chi$, since $\sigma^i \notin \langle \tau \rangle$ by assumption. Hence ϕ occurs with multiplicity greater than one in $\mathrm{Res}^G_H(\chi + \chi^{\sigma^{-i}})$, a contradiction, as both χ and $\chi^{\sigma^{-i}}$ are constituents of Φ.

Similarly, if $\phi^\gamma = \phi$ for some $\gamma \in \langle \sigma \rangle$, then $\gamma \in \langle \tau \rangle$, for otherwise ϕ occurs with multiplicity greater than one in $\mathrm{Res}^G_H(\chi + \chi^\gamma)$, while χ and χ^γ are distinct constituents of Φ, a contradiction. By the definition of β_1 ϕ and $\overline{\phi}$ are in different $\langle \sigma \rangle$-orbits, so that ϕ is an irreducible constituent of β. Since $\mathrm{Res}^G_H(\chi) - \beta_1$ is not faithful, $\mathrm{Res}^G_H(\chi) - \beta$ certainly is not, thus completing the proof of Theorem 4.

We suppose, then, that $\{\phi_i : 1 \leq i \leq t\}$ satisfying properties (i), (ii), and (iii) above can be found. We will produce a faithful submodule U of $\mathrm{Res}^G_H(V)$, an integer-valued generalized character, α', of H and a subgroup K of H with $[H:K] \leq 2$ such that:

(i) If $p = 2$, then $K = H$.

(ii) $\alpha'(h)^2 = [U : C_U(h)]$ for $h \in K$, $\alpha'(h)^2 = [U : C_U(h)]/p$ for $h \in H \setminus K$.

Once we have established that α' exists, we may complete the proof of Theorem 4 as follows:

Notice that for $h \in H^{\#}$, $\alpha'(h)$ is divisible by p unless p is odd, $h \in H \setminus K$, and $|C_U(h)| = |U|/p$. If $K \neq H$, we let λ denote the linear character of H whose kernel is K. For any $h \in H$, $|UC_V(h)| \leq |V|$, so that $[U:C_U(h)] \leq [V:C_V(h)]$ (with equality if and only if $[V,h] \leq U$). Hence $\alpha'(h)^2 \leq [V:C_V(h)]$ for each $h \in H$. Since $p \nmid \alpha'(1)$, it follows from Lemma 1 of [12] (and the remarks following) that we have $k(GV) \leq |V|$ (contrary to the hypothesis), unless perhaps p is odd and there is some $h \in H \setminus K$ with $|C_U(h)| = |U|/p$. Hence we may assume that p is odd and that $|C_U(h)| = |U|/p$ for some $h \in H \setminus K$.

Let $\gamma = \alpha' + \lambda\alpha'$. Then $\gamma(h) = 2\alpha'(h)$ for $h \in K$, while γ vanishes identically on $H \setminus K$. Hence $\gamma(h)$ is an integer multiple of p for each $h \in H^{\#}$, while $\gamma(1) = 2\alpha'(1)$, so $p \nmid \gamma(1)$.

Evidently, $HV = C_{GV}(v)$. For each generator, w, of $\langle v \rangle$ we define a class function $\Gamma^{(w)}$ of GV via:

$$\Gamma^{(w)}(x) = |C_V(h)|\gamma(h) \text{ if } x \text{ is conjugate to } hw \text{ for some } h \in H, \qquad 0 \text{ otherwise.}$$

We note that $\Gamma^{(w)} = \mathrm{Ind}_{HV}^{GV}(\mu^{(w)})$, where

$$\mu^{(w)} = \sum_{\phi \in \mathrm{Irr}(HV)} m_\phi\big(\phi(w^{-1})/\phi(1)\big)\phi$$

and

$$\mathrm{Ind}_H^{HV}(\gamma) = \sum_{\phi \in \mathrm{Irr}(HV)} m_\phi \phi.$$

In particular, $\Gamma^{(w)}$ is an algebraic integer combination of characters of GV.

The above description of $\Gamma^{(w)}$ allows us to deduce that for each irreducible character ϕ of GV, $\langle \Gamma^{(w)}, \phi \rangle = (1/|H|)\sum_{h \in H}\gamma(h)\phi(h^{-1}w^{-1})$. Since $p \nmid |H|\phi(1)\gamma(1)$, and since $p|\gamma(h)$ for all $h \in H^{\#}$, this inner product is certainly not zero. We also note that for each such ϕ, $\{\langle \Gamma^{(w)}, \phi \rangle : \langle w \rangle = \langle v \rangle\}$ is closed under algebraic conjugation.

For each generator w, of $\langle v \rangle$ we may write $\Gamma^{(w)} = \Gamma_0^{(w)} + \Gamma_1^{(w)}$, where $\Gamma_i^{(w)}(x) = \lambda^i(h)|C_V(h)|\alpha'(h)$ if x is conjugate to hw for some $h \in H$, 0 otherwise.

For each such w, every irreducible character, ϕ, of GV occurs with non-zero multiplicity in at least one of the $\Gamma_i^{(w)}$, and by remarks similar to those above, each $\langle \Gamma_i^{(w)}, \phi \rangle$ is an algebraic integer. Furthermore, for each i, and each generator, w, of $\langle v \rangle$, $\langle \Gamma_i^{(w)}, \phi \rangle$ is an algebraic conjugate of $\langle \Gamma_i^{(v)}, \phi \rangle$, so that for each i, $\langle \Gamma_i^{(v)}, \phi \rangle$ is non-zero if and only if each $\langle \Gamma_i^{(w)}, \phi \rangle$ is non-zero.

Let S_i denote the set of irreducible characters of GV which occurs with non-zero multiplicity in $\Gamma_i^{(v)}$. For $\mu \in S_i$, $\{\langle \Gamma_i^{(w)}, \mu \rangle : \langle w \rangle = \langle v \rangle\}$ is a set of algebraic integers closed under algebraic conjugation, so the arithmetic–geometric mean inequality yields $\sum_{\{w\,:\,\langle w\rangle=\langle v\rangle\}}|\langle\Gamma_i^{(2)},\mu\rangle|^2\geq\phi(|\langle v\rangle|)$, where ϕ denotes Euler's function.

For each i and each generator, w, of $\langle v\rangle$, we see that:

$$\begin{aligned}\langle\Gamma_i^{(w)},\Gamma_i^{(w)}\rangle &= |H|^{-1}\sum_{h\in H}|C_V(h)|\alpha'(h)^2\\ &= |H|^{-1}\sum_{h\in K}|C_V(h)|[U:C_U(h)]\\ &\qquad + |H|^{-1}\sum_{h\in H\setminus K}|C_V(h)|\frac{[U:C_U(h)]}{p}\\ &\leq \frac{|V|}{2}+\frac{|V|}{2p}\\ &= \left(\frac{p+1}{2p}\right)|V|.\end{aligned}$$

Hence we obtain (for each i)

$$\left(\frac{p+1}{2p}\right)|V|\phi(|\langle v\rangle|)\geq\sum_{\{w\,:\,\langle w\rangle=\langle v\rangle\}}\sum_{\mu\in S_i}|\langle\Gamma_i^{(w)},\mu\rangle|^2\geq|S_i|\phi(|\langle v\rangle|),$$

so that $|S_i|\leq((p+1)/2p)|V|$ for each i.

For each generator, w, of $\langle v\rangle$, we also see that

$$\langle\Gamma_0^{(w)}-\Gamma_1^{(w)},\Gamma_0^{(w)}-\Gamma_1^{(w)}\rangle=|H|^{-1}\sum_{h\in H\setminus K}4|C_V(h)|\frac{[U:C_U(h)]}{p}\leq\frac{2|V|}{p}.$$

Arguing as above, but with $\{\Gamma_0^{(w)}-\Gamma_1^{(w)}:\langle w\rangle=\langle v\rangle\}$, we deduce that $\sum_{\{w\,:\,\langle w\rangle=\langle v\rangle\}}\langle\Gamma_0^{(w)}-\Gamma_1^{(w)},\Gamma_0^{(w)}-\Gamma_1^{(w)}\rangle\leq(2|V|/p)\phi(|\langle v\rangle|)$, and then that at most $2|V|/p$ irreducible characters of GV occur with non-zero multiplicity in $\Gamma_0^{(v)}-\Gamma_1^{(v)}$. In particular, we conclude that $(|S_1\setminus S_0|+|S_0\setminus S_1|)\leq 2|V|/p$.

Now we have

$$\begin{aligned}k(GV) &= |S_0\cup S_1| = \frac{1}{2}\big[|S_0|+|S_1|+|S_1\setminus S_0|+|S_0\setminus S_1|\big]\\ &\leq \frac{1}{2}\left[\left(\frac{p+1}{2p}\right)|V|+\left(\frac{p+1}{2p}\right)|V|+\frac{2|V|}{p}\right]\\ &= \left(\frac{p+3}{2p}\right)|V|.\end{aligned}$$

Since p is odd, we have $k(GV)\leq|V|$, a contradiction.

It remains, then, to construct the submodule U, and the generalized character α', given the existence of $\phi_1, \phi_2, \ldots, \phi_t$ satisfying conditions (i)–(iii).

We label: for $1 \le i \le r$, ϕ_i satisfies condition (iii)(a); for $r+1 \le i \le s$, ϕ_i satisfies condition (iii)(b), but not (iii)(a); and for $s+1 \le i \le t$, ϕ_i satisfies condition (iii)(c), but neither condition (iii)(a) nor condition (iii)(b).

For $1 \le i \le r$, let V_i be an irreducible $GF(p)H$-module whose Brauer character has ϕ_i as a constituent. Then $\mathrm{Res}_H^G(V)$ has a submodule U_i which is isomorphic to $V_i \oplus V_i$. By the results of Knörr [4], there is a generalized character δ_i of H defined via $\delta_i(h) = [V_i : C_{V_i}(h)]$ for each $h \in H$. We note that $\delta_i(h)^2 = [U_i : C_{U_i}(h)]$ for each $h \in H$, δ_i is integer valued, and that $\delta_i(h)$ is divisible by p unless h acts trivially on U_i.

For $r+1 \le i \le s$, we choose $\gamma_i \in \mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q})$ so that $\phi_i^{\gamma_i}$ is an irreducible constituent of ψ in a different $\langle \sigma \rangle$-orbit from ϕ_i. We let V_i be an irreducible $GF(p)H$-module whose Brauer character has ϕ_i as a constituent, $V_i^{\gamma_i}$ be an irreducible $GF(p)H$-module whose Brauer character has $\phi_i^{\gamma_i}$ as a constituent. Then $\mathrm{Res}_H^G(V)$ has a submodule U_i which is isomorphic to $V_i \oplus V_i^{\gamma_i}$. Again, we define the generalized character δ_i of H via $\delta_i(h) = [V_i : C_{V_i}(h)]$ for each $h \in H$. Again we see that $\delta_i(h)^2 = [U_i : C_{U_i}(h)]$ for each $h \in H$, that δ_i is integer-valued and that $\delta_i(h)$ is divisible by p unless h acts trivially on U_i.

For $s+1 \le i \le t$, $\mathrm{Res}_H^G(V)$ has an irreducible self-dual submodule U_i such that the Brauer character afforded by U_i has ϕ_i as a constituent. We note that when $i \ne j$, U_i and U_j have no common composition factor, so that $U = \oplus_{i=1}^t U_i$ is a submodule of $\mathrm{Res}_H^G(V)$. Furthermore, U is a faithful $GF(p)H$-module. We set $W = \oplus_{i=s+1}^t U_i$, and we write $W = X \oplus Y$, where X admits an H-invariant, non-degenerate, alternating form and Y admits an H-invariant, non-degenerate, symmetric form. If $p = 2$, then we assume that H acts trivially on Y, as we may.

Now X has even-dimension, say $2m$, over $GF(p)$. From Gow [3], there is a rational-valued generalized character, α, of H such that $\alpha(h)^2 = |C_X(h)|$ for each $h \in H$, and the class function γ of HX defined by $\gamma(u) = p^m \alpha(h)$ if u is conjugate to $h \in H$, $\gamma(u) = 0$ otherwise, is a generalized character of HX. Corresponding to γ, there is a generalized character, ζ, of H with $\zeta(h) = \gamma(h)/|C_X(h)|$ for each h in H.

Then $\zeta(h)^2 = [H : C_X(h)]$ for each h in H. Furthermore, $p \nmid \zeta(1)$, and for any $h \in H$ which acts non-trivially on X, $\zeta(h)$ is divisible by p.

If $p = 2$, or if $W = X$, we let θ be the trivial character of H, and take $K = H$. Otherwise, we let λ be the linear character of H afforded by the determinant of its action on Y, $K = \ker \lambda$. Then $[H : K] \le 2$, as $Y \cong Y^*$. We construct an integer-valued generalized character, θ, of H with $\theta(h)^2 = [Y : C_Y(h)]$ for $h \in K$, $\theta(h)^2 = [Y : C_Y(h)]/p$ for $h \in H \setminus K$.

From Gow [3, pp. 448–449], we know that when Y is even-dimensional over $GF(p)$, there is an integer-valued generalized character, ξ, of H with $\xi(h)^2 = |C_Y(h)|$ for $h \in K$, $p\xi(h)^2 = |C_Y(h)|$ for $h \in H \setminus K$. When Y is odd-dimensional over $GF(p)$, there is an integer-valued generalized character, ξ, of H with $\xi(h)^2 = p|C_Y(h)|$ for $h \in K$, $\xi(h)^2 = |C_Y(h)|$ for $h \in H \setminus K$.

In either case, if Y has dimension $2m$ or $2m+1$, respectively, we define the integer-valued generalized character, γ of HY via $\gamma(u) = p^m\xi(h)$ if u is conjugate to $h \in H$; 0 otherwise. There is a corresponding generalized character, θ, of H with $\theta(h) = \gamma(h)/|C_Y(h)|$ for $h \in H$. We see that $\theta(h)^2 = [Y : C_Y(h)]$ for $h \in K$, $\theta(h)^2 = [Y : C_Y(h)]/p$ for $h \in H \setminus K$, so that θ is the required generalized character.

Now we are ready to complete the proof of Theorem 4. We let α' be the generalized character $\theta\zeta\prod_{i=1}^{s}\delta_i$ of H. Then α' is integer-valued, and $\alpha'(h)^2 = [U : C_U(h)]$ for $h \in K$, $\alpha'(h)^2 = [U : C_U(h)]/p$ for $h \in H \setminus K$. Furthermore, $p \nmid \alpha'(1)$, and for $h \in H^\#$, $\alpha'(h)$ is divisible by p unless p is odd and $h \in H \setminus K$ with $|C_U(h)| = |U|/p$. Thus α' is the generalized character required to complete the proof of Theorem 4. Careful examination of the proof above shows that Theorem 2 can be sharpened:

COROLLARY 5. *Let p be a prime, G be a finite p'-group, V be a faithful irreducible $GF(p)G$-module. Suppose that for some $v \in V$, $\mathrm{Res}_H^G(V)$ has a faithful submodule U with $U \cong U^*$, where $H = C_G(v)$. Then $k(GV) \le |V|$. If equality holds then $V \cong V^*$ as $GF(p)H$-module and $[V, H] \le U$; furthermore, if U is a permutation module, then equality forms $\mathrm{Res}_H^G(V)$ to be a permutation module.*

Proof. If $[V, H] \not\le U$, then there is some $h \in H$ with $[V, h] \not\le U$, so that (as we remarked in the proof of Theorem 4), $[U : C_U(h)] < [V : C_V(h)]$. Hence in the argument relying on Lemma 1 of [12] we have $\langle \alpha', \alpha' \rangle < |V|$. In that case we obtain $k(GV) < |V|$.

If $[V, H] \le U$, then $\mathrm{Res}_H^G(V) = U \oplus T$, where H acts trivially on T. In that case $V \cong V^*$ as $GF(p)H$-module, and if U is a permutation module, then so is $\mathrm{Res}_H^G(V)$.

Remark. We consider that Theorem 4 indicates that the conditions under which the desired inequality $k(GV) \le |V|$ can be violated are extremely restrictive. However, if we take G be the semi-direct product of an extra-special group of order 27 and exponent 3 with $SL(2,3)$ (acting in the obvious manner), then G has an absolutely irreducible three-dimensional representation over $GF(7)$. Letting V denote the associated $GF(7)G$-module, we find (using the notation of Theorem 4) that $\mathrm{Res}_{C_G(v)}^G(\chi) - \beta$ is not faithful for any $v \in V$. However, the inequality $k(GV) \le |V|$ is not violated in this example, using (for example), the results of Knörr [5], since there is a vector $v \in V$ such that $C_G(v)$ is Abelian.

3. REGULAR ORBITS AND PERMUTATION SUMMANDS

We will be concerned in later sections with primes which satisfy:

Hypothesis 1. p is a prime with the property that whenever H is a finite p'-group, F is a finite field, of characteristic p and U is a faithful FH-module such that **either**

(a) For some prime q, $O_q(H)$ acts absolutely irreducibly on U, and every characteristic Abelian subgroup of $O_q(H)$ is central, **or**

(b) $E(H)$ is quasi-simple and acts absolutely irreducibly on U, then there is a vector $u \in U$ such that $\mathrm{Res}^H_{C_H(u)}(U)$ has a faithful permutation module as a summand.

In this section we will prove that all primes p with $p > 5^{30}$ satisfy hypothesis 1. To deal with case (b) above, we rely on a recent improvement by Liebeck [8] of Theorem 6 of Hall, Liebeck, and Seitz [4]:

THEOREM (Liebeck, [8]). *Let p be a prime with $p > 5^{30}$, G be a finite p'-group, V be a faithful $GF(p)G$-module such that G has no regular orbit on V and G has a quasi-simple normal subgroup H which acts irreducibly on V. Then $H \cong A_n$ for some integer n with $n < p$, and V has dimension $(n-1)$. Furthermore, $\mathrm{Res}^G_H(V)$ is isomorphic to the quotient of the "natural" n-dimensional permutation module for H by its trivial submodule.*

We draw a corollary to this result which explains its relevance for us.

COROLLARY 6. *Let p be a prime greater than 5^{30}, F be a finite field of characteristic p. Let G be a finite group such that $E = E(G)$ is quasi-simple. Let V be a faithful FG-module such that $\mathrm{Res}^G_E(V)$ is absolutely irreducible. Then there is a vector $v \in V$ such that $\mathrm{Res}^G_{C_G(v)}(V)$ has a faithful permutation module as a summand.*

Proof. Let σ be the matrix representation of G afforded by V. Let k be the extension field of $GF(p)$ generated by $\{\mathrm{trace}(g\sigma) : g \in G\}$. There is a kG-module U such that $V \cong U \otimes_k F$, and $\mathrm{Res}^G_E(U)$ is also absolutely irreducible. Hence we may suppose that $k = F$, and do so. Then there is an irreducible $GF(p)G$-module W such that V is isomorphic to a summand of $W \otimes_{GF(p)} F$ and $F \cong \mathrm{End}_{GF(p)G}(W)$. Furthermore, $\mathrm{Res}^G_E(W)$ is irreducible, and the permutation actions of G on vectors of V, W, respectively, are equivalent. We may suppose that G has no regular orbit on V, hence has no regular orbit on W. Then Liebeck's theorem yields $E \cong A_n$ for some integer $n < p$, and $W = V$ is absolutely irreducible of dimension $n - 1$. Let $Z = Z(G)$ ($= C_G(E)$ under the hypotheses of the corollary), and let e be the exponent of G/Z. For any $g \in G$ with $|C_V(g)| > 1$ we must have $g^e = 1_G$. Hence no coset of Z in G can contain more than e elements g for which $|C_V(g)| > 1$. Since G has no regular orbit on V, we have $V = \bigcup_{g \in G^\#} C_V(g)$, so that $p^{n-1} < e[G:Z]p^{n-2}$, and $p < e[G:Z]$. Certainly, then, $n > 6$, as $p > 5^{30}$. Thus $\mathrm{Aut}(E) \cong S_n$, and we may identify V with $\{\sum_{i=1}^n \alpha_i v_i : \alpha_i \in GF(p), \sum_{i=1}^n \alpha_i = 0\}$, where $\{v_i : 1 \le i \le n\}$ is linearly independent, and for each $g \in G$ there is some $\lambda \in GF(p)^\#$ such that λg permutes $\{v_i : 1 \le i \le n\}$.

Let $u = (n-1)v_1 - \sum_{i=2}^n v_i$. If $ug = u$ for some $g \in G$, then g must fix v_1 and permute $\{v_1 - v_i : 2 \le i \le n\}$. Hence $C_G(u) \cong A_{n-1}$ or S_{n-1}, and $\mathrm{Res}^G_{C_G(u)}(V)$ is isomorphic to the natural permutation module.

To deal with case (a) of Hypothesis 1, we require some preparation.

LEMMA 7. *Let q be a prime, Q be a central product of the form ZE, where Z is a finite cyclic q-group and E is an extra-special q-group (of exponent q if q is odd). Suppose that $Q \lhd P$ with $P = Q\langle x \rangle$ and $|\langle x \rangle| = q$. Suppose that P has a faithful complex irreducible character χ of degree q^n, where $|E| = q^{2n+1}$. Then $\langle \mathrm{Res}^P_{\langle x \rangle}(\chi), 1 \rangle \le (q^n + q^{n-1})/2$.*

Proof. We may, and do, suppose that $Q = \Omega_1(Q)$ if q is odd, $Q = \Omega_2(Q)$ if $q = 2$. We first claim that it suffices to deal with the case that $C_Q(x)$ is Abelian. Suppose that that case has been dealt with, but that $C_Q(x)$ is non-Abelian. Then $C_Q(x)$ contains an extra-special subgroup T of order q^3, and $Q = TC_Q(T)$. Let $P_0 = \langle x \rangle C_Q(T)$. Then $\chi(x) = q\mu(x)$ for some irreducible character μ of degree q^{n-1} of P_0, and $\langle \mathrm{Res}^P_{\langle x \rangle}(\chi), 1 \rangle = q\langle \mathrm{Res}^{P_0}_{\langle x \rangle}(\mu), 1 \rangle$. Since $P_0 = Q_0\langle x \rangle$, where $Q_0 = C_Q(T) \lhd P_0$, and since Q_0 has structure analogous to that of Q, our first claim is established. Hence we assume that $C_Q(x)$ is Abelian from now on. We may also suppose that $\chi(x) \neq 0$, so that, in particular, $x \notin Q$.

The maximum order of an Abelian subgroup of E is q^{n+1}, so that $|C_Q(x)| \le q^{n+1}, |C_P(x)| \le q^{n+2}$ when $|Z(Q)| = q$, while if $|Z(Q)| = 4$ we obtain $|C_Q(x)| \le q^{n+2}, |C_P(x)| \le q^{n+3}$. Suppose that $Z(Q)$ has order q.

Then there are (at least) $q - 1$ algebraic conjugates of χ, each of which may be multiplied by the q linear characters of P/Q, so we deduce that $\sum_{i=1}^{q-1} |\chi(x^i)|^2 < q^{n+1}$. Hence $\|\mathrm{Res}^P_{\langle x \rangle}(\chi)\|^2 < (1/q)(q^{2n} + q^{n+1}) = q^{2n-1} + q^n$. If $\langle \mathrm{Res}^P_{\langle x \rangle}(\chi), 1 \rangle > (q^n + q^{n-1})/2$, we obtain $((q^n + q^{n-1})/2)^2 < q^{2n-1} + q^n$ which yields $q = 2$, $n \le 3$ or $q = 3$, $n = 1$. If $n = 1$ we have

$\langle \mathrm{Res}^P_{\langle x\rangle}(\chi), 1\rangle \leq q - 1 \leq (q+1)/2$. If $q = n = 2$, we have $\langle \mathrm{Res}^P_{\langle x\rangle}(\chi), 1\rangle \leq 3 = (2^2 + 2^1)/2$. If $n = 3$ and $q = 2$, then $\langle \mathrm{Res}^P_{\langle x\rangle}(\chi), 1\rangle > (2^3 + 2^3)/2$ forces $\chi(x) = 6$, a contradiction as $|C_P(x)| \leq 32$.

Suppose then that $Z(Q)$ has order 4. Then we have $|C_P(x) \leq 2^{n+3}$. Now there are (at least) two algebraic conjugates of χ which each may be multiplied by the two linear characters of P/Q, so we may conclude that $\chi(x)^2 < 2^{n+1}$. We may argue to a contradiction as above, except that we must also note that $\bar{\chi} \neq \chi$ when $n = 3$, while $|C_P(x)| \leq 64$.

THEOREM 8. *Let p be a prime, F be a finite field of characteristic p with $|F| \geq 2^{27}$, G be a finite p'-group, V be a faithful FG-module. Suppose that, for some prime q, G has a normal q-subgroup Q which acts absolutely irreducibly on V, and all of whose characteristic Abelian subgroups are central. Then G has a regular orbit on V.*

Proof. Let r denote $|F|$. Since Q acts absolutely irreducibly on V, every characteristic Abelian subgroup of Q is central in G. We may, and do, suppose that G contains all non-zero scalar transformations. Then $F(G) = ZQ$, where $Z = Z(G) \cong F^{\#}$, and $E(G) = 1_G$. There is an integer n such that $\dim_F(V) = q^n$ and $G/F(G)$ is isomorphic to a subgroup of $\mathrm{Sp}(2n, q)$. We may, and do, suppose that $Q = \Omega_1(Q)$ is q is odd, $Q = \Omega_2(Q)$ if $q = 2$.

Suppose that G has no regular orbit on V. Then $V = \bigcup_{g \in G^{\#}} C_V(g)$. We claim that $\dim_F(C_V(g)) \leq (q^n + q^{n-1})/2$ for each $g \in G^{\#}$. Let χ be Brauer character of G afforded by V, so by hypothesis χ is a complex irreducible character of G. To establish the inequality in the claim, it suffices to consider the case that g has prime order. By Lemma 7, we may suppose that g has prime order $s \neq q$. Applying Glauberman correspondence within the group $Q\langle g\rangle$, there is an irreducible character, μ, of $C_Q(g)$, there is a sign ϵ, and there is an sth root of unity, ω, such that $\chi(g) = \epsilon\omega\mu(1)$. We may suppose that $g \notin Z(G)$, so that $\mu(1) \leq q^{n-1}$. Hence $\langle \mathrm{Res}^G_{\langle g\rangle}(\chi), 1\rangle \leq (1/s)[q^n + (s-1)q^{n-1}] \leq (q^n + q^{n-1})/2$.

Using elementary estimate $|\mathrm{Sp}(2n, q)| < q^{2n^2+n}$ and the fact that $|Z(G)| = r - 1$, we obtain

$$|V| = r^{q^n} < \sum_{g \in G^{\#}} |C_V(g)| < |G| r^{(q^n + q^{n-1})/2} < r \cdot q^{2n^2+3n} r^{(q^n+q^{n-1})/2},$$

so that (except in the cases $n = 1$, $q < 4$, or $q = n = 2$), we obtain $\log(r) < ((4n^2 + 6n)/(q^n - q^{n-1} - 2))\log(q)$, which leads easily (via elementary calculus) to $r < 2^{27}$, contrary to hypothesis.

In the exceptional cases, the more delicate argument used during the proof of Lemma 7 leads this time to $r^{q^n} < e[G:Z]r^{((q^n+q^{n-1})/2)}$, where $Z = Z(G)$ and e is the exponent of G/Z. Thus $r^{(q^n - q^{n-1})/2} < e[G:Z]$. In the cases $n = 1$, $q = 2$, $n = 1$, $q = 3$, and $n = q = 2$ we respectively obtain $[G:Z] < 32$, $[G:Z] < 243$, and $[G:Z] < 2^{14}$, so in each case we easily obtain $r < 2^{27}$, contrary to hypothesis.

Corollary 6 and Theorem 8 establish that all primes p with $p > 5^{30}$ satisfy Hypothesis 1.

4. CLIFFORD THEORY AND THE VECTOR v

In this section, we use Clifford-theoretic reductions to complete the proof of Theorem 3. We collect some straightforward lemmas together for the convenience of the reader. All are well known and easily proved.

LEMMA 9. *Let p be a prime, F be a finite field of characteristic p, H be a finite p'-group, U and V be FH-modules, k be a finite extension field of F. Then if $V \otimes_F k$ has a summand isomorphic to $U \otimes_F k$, V has a summand isomorphic to U.*

LEMMA 10. *Let p be a prime, F be a finite field of characteristic p, H be a finite p'-group, V be a faithful irreducible FH-module, $k = \mathrm{End}_{FH}(V)$. Then the irreducible summands of $V \otimes_F k$ are absolutely irreducible, and if U is any one of them, the permutation actions of G on vectors of V, U, respectively, are equivalent.*

LEMMA 11. *Let p be a prime, F be a finite field of characteristic p, k be a finite extension of F, H be a finite p'-group. Let V be a finite-dimensional kH-module such that $\mathrm{trace}_V(h) \in F$ for all $h \in H$. Then there is an FH-module U with $V \cong U \otimes_F k$.*

The main result of this section is somewhat stronger than Theorem 3.

THEOREM 12. *Let p be a prime which satisfies hypothesis* 1 *of Section* 3. *Let k be a finite field of characteristic p, G be a finite p'-group, U be an absolutely irreducible faithful kG-module. Then there is a vector $u \in U$ such that $\mathrm{Res}^G_{C_G(u)}(U)$ has a summand which is a faithful permutation module.*

Proof. Suppose that the theorem is false, and choose (G, U, k) to violate the theorem with $\dim_k(U)$ as small as possible. We assume, as we may, that G contains all non-zero scalar transformations of U, regarding G as a subgroup of $GL(U)$.

We first claim that U is primitive. For if $U \cong \mathrm{Ind}^G_H(W)$, where $H < G$ and W is a kH-module, then W is absolutely irreducible. The minimality of $\dim_k(U)$ allows us to conclude that there is some $w \in W$ such that $\mathrm{Res}^H_{C_H(w)}(W)$ has a summand which is a permutation module, say X, with $C_H(w) \cap C_H(X) = C_H(W)$. Let T be a right transversal to H in G. Then, as k-vector space, $U = \oplus_{t\in T} Wt$. Let $u = \sum_{t\in T} wt$. Then it is routine to verify that $\oplus_{t\in T} Xt$ is a faithful permutation module for $C_G(u)$, and is a summand of $\mathrm{Res}^G_{C_G(u)}(U)$, contrary to hypothesis.

We next claim that whenever $N \lhd G$, all irreducible summands of $\mathrm{Res}^G_N(U)$ are absolutely irreducible. Suppose otherwise, and choose $N \lhd G$ to be maximal subject to: $\mathrm{Res}^G_N(U)$ has an irreducible summand, W, which is not absolutely irreducible. As U is a primitive kG-module, we see easily that $\mathrm{End}_{kN}(U) \cong M_d(\mathrm{End}_{kN}(W))$, where $\dim_k(U) = d\dim_k(W)$, and that $Z(\mathrm{End}_{kN}(U)) \cong \mathrm{End}_{kN}(W)$, a finite extension of k. Let $L = Z(\mathrm{End}_{kN}(U))$, $M = C_G(L)$. Then $M \lhd G$ and $N \le M$. Let $t = [L:k]$.

Now $W \otimes_k L$ is a direct sum of t pairwise non-isomorphic, but Galois conjugate, absolutely irreducible LN-modules, and G/M is isomorphic to a subgroup of $\mathrm{Gal}(L/k)$. Let $W \otimes_k L = \oplus_{i=1}^t W_i$, where the W_i are irreducible LN-modules (each of which is faithful). By definition of M, $Z(\mathrm{End}_{kN}(U)) \subseteq \mathrm{End}_{kM}(U) \subseteq \mathrm{End}_{kN}(U)$, so that $Z(\mathrm{End}_{kN}(U)) \subseteq Z(\mathrm{End}_{kM}(U))$. Hence $Z(\mathrm{End}_{kM}(U)) \not\cong k$, so the argument used above for N tells us that $\mathrm{Res}^G_N(U)$ has an irreducible summand which is not absolutely irreducible. The maximal choice of N forces $N = M$.

Since $[G:M] \le t$, and $\mathrm{Res}^G_M(U \otimes_k L) \cong d \oplus_{i=1}^t W_i$, we deduce from Clifford's theorem and Lemma 11 that $[G:M] = t$, and that $\mathrm{Ind}^G_M(W_1) \cong U \otimes_k L$. Thus $\mathrm{Res}^G_M(U) = W$. By the minimality of $\dim(U)$, there is a vector $w_1 \in W_1$ such that $\mathrm{Res}^M_{C_M(w_1)}(W_1)$ has a summand, X_1 say, which is faithful permutation module. By Lemma 10, there is a vector $w \in W$ with $C_M(w_1) = C_M(w)$.

Now $U \otimes_k L \cong \mathrm{Ind}^G_M(W_1)$, so by Mackey decomposition, $\mathrm{Res}^G_{C_G(w)}(U \otimes_k L) \cong \mathrm{Ind}^{C_G(w)}_{C_M(w)}(\mathrm{Res}^M_{C_M(w)}(W_1)) \oplus Y$ for some $LC_G(w)$-module Y. Thus $\mathrm{Res}^G_{C_G(w)}(U \otimes_k L) \cong \mathrm{Ind}^{C_G(w)}_{C_M(w)}(X_1) \oplus Y'$ for some $LC_G(w)$-module Y'. Using Lemma 9, $\mathrm{Res}^G_{C_G(w)}(U)$ has a summand which is a faithful permutation module, contrary to hypothesis.

We next claim that whenever $N \lhd G$ with $N \not\le Z(G)$, $\mathrm{Res}^G_N(U)$ is irreducible. If possible, choose $N \lhd G$ with $N \not\le Z(G)$ such that $\mathrm{Res}^G_N(U)$ has an irreducible constituent, W say, with $\dim_k(W) < \dim_k(U)$. Let $\sigma: N \to GL(W)$ be the representation afforded by W. Since U is primitive and W is absolutely irreducible, there is (as usual) for each $g \in G$ an element $\zeta_g \in GL(W)$ (unique up to non-zero scalar multiples) such that for all $n \in N$, $\zeta_g^{-1}(n\sigma)\zeta_g = (g^{-1}ng)\sigma$. Let T be a transversal to N in G (with $1_G \in T$), and arrange so that $\zeta_{tn} = \zeta_t(n\sigma)$ for all $t \in T, n \in N$. For each $g, h \in G$ there is $\alpha(g,h) \in k^*$ with $\zeta_g\zeta_h = \alpha(g,h)\zeta_{gh}$. We set $\tilde{G} = \{(g,z): g \in G, z \in k\}$ with product $(g_1,z_1)(g_2,z_2) = (g_1g_2, \alpha(g_1, g_2)z_1z_2)$. Then $\tilde{G}$ is a finite group with $\tilde{G}/\tilde{Z} \cong G$, where $\tilde{Z} = \{(1,z): z \in k^*\} \le Z(\tilde{G})$. Let $\tilde{N} = \{(n,1): n \in N\}$. Then $\tilde{N} \lhd \tilde{G}$, and $\tilde{N} \cong N$.

We may endow W with the structure of a $k\tilde{G}$-module by defining $\tilde{\sigma}: \tilde{G} \to GL(W)$ via $(g, z)\tilde{\sigma} = z\zeta_g$ for all $g \in G, z \in k^*$. Identifying N with $\tilde{N}$, this extends the original action of N on W. In particular, W is an absolutely irreducible $k\tilde{G}$-module. We now view U as a $k\tilde{G}$-module on which $\tilde{Z}$ acts trivially, using the action of G.

There is a finite extension, L, of k such that $U \otimes_k L$ "factorizes" as $(U \otimes_k L) \cong (W \otimes_k L) \otimes \tilde{X}$ for some (absolutely irreducible) $L\tilde{G}$-module $\tilde{X}$, and $\tilde{N}$ acts trivially on $\tilde{X}$. Now $\{n\sigma : n \in N\}$ spans $\mathrm{End}_k(W)$ as W is an absolutely irreducible kN-module. For any $\tilde{g} \in \tilde{G}$, we may choose $\tilde{n} \in \tilde{N}$ so that $\mathrm{trace}_{W \otimes_k L}(\tilde{g}\tilde{n}) \neq 0$. Then $\mathrm{trace}_{\tilde{X}}(\tilde{g}) = \mathrm{trace}_{U \otimes_k L}(\tilde{g}\tilde{n}) / \mathrm{trace}_{W \otimes_k L}(\tilde{g}\tilde{n}) \in k$. By Lemma 11, there is a $k\tilde{G}$-module X with $\tilde{X} \cong X \otimes_k L$. Hence $U \cong W \otimes X$ as $k\tilde{G}$-module, and X is absolutely irreducible.

By the minimality of $\dim(U)$, there are vectors $w \in W$, $x \in X$ such that $\mathrm{Res}^{\tilde{G}}_{C_{\tilde{G}}(w)}(W)$ has a summand Y_1 which is a permutation module with $C_{\tilde{G}}(Y_1) \cap C_{\tilde{G}}(w) = C_{\tilde{G}}(W)$ and $\mathrm{Res}^{\tilde{G}}_{C_{\tilde{G}}(x)}(X)$ has a summand Y_2 which is a permutation module with $C_{\tilde{G}}(Y_2) \cap C_{\tilde{G}}(x) = C_{\tilde{G}}(X)$. Let $u = w \otimes x$.

If $(g, 1) \in \tilde{G}$ fixes $w \otimes x$ then there is some $\lambda \in k^*$ such that $w(g, 1) = \lambda w$, $x(g, 1) = \lambda^{-1}x$. Hence $\lambda^{-1}(g, 1) \in C_{\tilde{G}}(w)$, $\lambda(g, 1) \in C_{\tilde{G}}(x)$, so that $\lambda^{-1}(g, 1)$ permutes the distinguished basis of Y_1, $\lambda(g, 1)$ permutes the distinguished basis of Y_2. Thus $(g, 1)$ permutes the distinguished basis of $Y_1 \otimes Y_2$. Furthermore, if $(g, 1)$ fixes (elementwise) the distinguished basis of $Y_1 \otimes Y_2$, then $\lambda^{-1}(g, 1)$ fixes (elementwise) the distinguished basis of Y_1, $\lambda(g, 1)$ fixes (elementwise) the distinguished basis of Y_2. Thus $\lambda^{-1}(g, 1) \in C_{\tilde{G}}(W)$ and $\lambda(g, 1) \in C_{\tilde{G}}(X)$ so that $(g, 1) \in C_{\tilde{G}}(W \otimes X)$. Hence $Y_1 \otimes Y_2$ is a summand of $\mathrm{Res}^{G}_{C_G(u)}(W \otimes X)$ which is a faithful permutation module for $C_G(u)$, contrary to hypothesis, as $U \cong W \otimes X$.

Next, we claim that $F(G) \leq Z(G)$, and that $E(G) = E$ is a central product of a single G-conjugacy class of components, but E is not quasi-simple.

If there is a prime q such that $O_q(G) \not\leq Z(G)$, then $O_q(G)$ acts absolutely irreducibly on U and every characteristic Abelian subgroup of $O_q(G)$ is central in G, so hypothesis 1 of Section 3 implies that there is a vector $u \in U$ such that $\mathrm{Res}^{G}_{C_G(u)}(U)$ has a faithful submodule which is a permutation module, a contradiction. Hence $F(G) \leq Z(G)$, so that $E = E(G) \not\leq Z(G)$. Now E acts absolutely irreducibly on U, so Hypothesis 1 of Section 3 ensures that E cannot be quasi-simple. Since every non-central normal subgroup of G acts absolutely irreducibly on U, E must be the central product of a single G-conjugacy class of components.

Now we proceed to a final contradiction. We may write $E = L_1 L_2 \cdots L_t$, where $t > 1$ and the L_i are distinct G-conjugate components. We set $M_1 = N_G(L_1)$, and let $\{g_1 : 1 \leq i \leq t\}$ be a right transversal to M_1 in G, labelled so that $L_1^{g_i} = L_i$ for each i (and we take $g_1 = 1_G$). We reproduce the now standard argument that the given representation, σ say, of G on U is tensor-induced (as a projective representation) from a projective representation of M_1. Since $\mathrm{Res}_E^G(U)$ is absolutely irreducible, we see easily that $\mathrm{Res}_E^G(U) \cong \otimes_{1=t}^t U_i$, where U_1 is an absolutely irreducible submodule of $\mathrm{Res}_{L_1}^G(U)$ and where $U_i = U_1 g_i$ is an absolutely irreducible kL_i-module for $2 \le i \le t$. Since $\mathrm{Res}_E^G(U)$ is absolutely irreducible, we note that $g\sigma$ is the unique (up to non-zero scalar multiples) linear transformation $T \in \mathrm{End}_k(U)$ with the property that $T^{-1}(x\sigma)T = (g^{-1}xg)\sigma$ for all $x \in E$.

Since $\mathrm{Res}_{L_1}^G(U)$ is homogeneous, M_1 preserves the isomorphism type of U_1, and for each $m \in M_1$ there is a unique (up to non-zero scalar multiples) element $\zeta(m) \in \mathrm{End}_k(U_1)$ with $\zeta(m)y\tau\zeta(m)^{-1} = (mym^{-1})\tau$ for all $y \in L_1$, where τ is the given representation of L_1 on U_1.

Choose $h \in G$. Let $\gamma \in S_t$ be defined by $M_1 g_{i\gamma} = M_1 g_i h$ for $1 \le i \le t$. There is a unique linear transformation $T_h \in \mathrm{End}_k(U)$ specified by: for $1 \le i \le t$ and for all $u_1 \in U_1$, $(u_1 g_i)T_h = u_1 \zeta(g_i h g_{i\gamma}^{-1})g_{i\gamma}$ and extending this action in the obvious fashion to tensors. A routine computation verifies that $(T_h)^{-1}x\sigma T_h = (h^{-1}xh)\sigma$ for all $x \in E$, so that T_h is a non-zero scalar multiple of $h\sigma$. This establishes that σ is tensor induced (as a projective representation) from the above projective representation of M_1 on U_1.

As before, we may construct a central extension $\tilde{M}_1$ of M_1, having a central subgroup $\tilde{Z} \cong k^*$ with $\tilde{M}_1/\tilde{Z} \cong M_1$ and having a normal subgroup $\tilde{L}_1 \cong L_1$ (which may be identified with L_1) such that (with this identification), τ extends to a genuine representation of $\tilde{M}_1$ on U_1.

Since $\tilde{L}_1$ acts absolutely irreducibly on U_1 Hypothesis 1 of Section 3 allows us to conclude that there is a vector $u_1 \in U_1$ such that $\mathrm{Res}_{C_{\tilde{M}_1}(u_1)}^{\tilde{M}}(U_1)$ has a summand, X_1 say, which is a permutation module with $C_{\tilde{M}_1}(u_1) \cap C_{\tilde{M}_1}(X_1) = C_{\tilde{M}_1}(U_1)$. Even if $C_{\tilde{M}_1}(u_1) = C_{\tilde{M}_1}(U_1)$, we may, and do, assume that $\dim_k(X_1) \ge 2$.

For $2 \le i \le t$, we set $u_i = u_1 g_i \in U_i$ and $X_i = X_1 g_i \le U_i$. We let $u = u_1 \otimes u_2 \otimes \cdots \otimes u_t$. We claim that $X_1 \otimes X_2 \cdots \otimes X_t$ is a submodule of $\mathrm{Res}_{C_G(u)}^G(U)$ which is a faithful permutation module.

If $h \in G$ satisfies $uh = u$, then there are scalars $\lambda_1, \dots, \lambda_t \in k^*$ and there is a permutation $\gamma \in S_t$ such that $\prod_{i=1}^t \lambda_i = 1$ and $u_1 g_i h = \lambda_i g_{i\gamma}$ for each i. Then for each i, $\lambda_i^{-1}(g_i h g_{i\gamma}^{-1}, 1) \in C_{\tilde{M}_1}(u_1)$, so it permutes the distinguished basis of X_1. Hence $\lambda_i^{-1}h$ sends the distinguished basis of X_i to the distinguished basis of $X_{i\gamma}$. Since $\prod_{i=1}^t \lambda_i = 1$, h permutes the distinguished basis of $X_1 \otimes X_2 \otimes \cdots \otimes X_t$. If h fixes this basis elementwise, we first note that for each i, $\lambda_i^{-1}(g_i h g_{i\gamma}^{-1}, 1)$ acts trivially on U_1. For otherwise there is a value of i such that the distinguished basis of X_1 contains a vector y which is not fixed by $\lambda_i^{-1}(g_i h g_{i\gamma}^{-1}, 1)$ (hence it is not sent to a scalar multiple of itself either). In that case, the distinguished basis vector $yg_1 \otimes yg_2 \otimes \cdots \otimes yg_t$ of $X_1 \otimes X_2 \otimes \cdots \otimes X_t$ is not fixed by h, contrary to assumption. Next we claim that γ is the identity permutation of S_t. For if $i\gamma \neq i$ for some i, we choose distinct vectors x, y from the distinguished basis of X_1 and we let $w = yg_1 \otimes \cdots \otimes yg_{i-1} \otimes xg_i \otimes yg_{i+1} \cdots \otimes yg_t$, a distinguished basis vector for $X_1 \otimes X_2 \otimes \cdots \otimes X_t$. Then wh is a distinguished basis vector for $X_1 \otimes X_2 \otimes \cdots \otimes X_t$ with $xg_{i\gamma}$ in position $i\gamma$, so certainly $wh \neq w$, contrary to assumption. Now we know that for $1 \leq i \leq t$, $\lambda_i^{-1}(g_i h g_i^{-1}, 1)$ acts trivially on U_1, so that $(h, 1)$ acts as multiplication by λ_i on $U_i = U_1 g_i$ for each i. Since $\prod_{i=1}^{t} \lambda_i = 1$, h acts trivially on U, as required to complete the proof of Theorem 12.

Now we can state a slightly sharper version of Theorem 3 (which implies the version stated in the introduction by the results of Section 3).

THEOREM 3. *Let p be a prime which satisfies Hypothesis* 1 *of Section* 3. *Let G be a finite group of order prime to p, and V be faithful irreducible $GF(p)G$-module. Then there is a vector $v \in V$ such that* $\operatorname{Res}^G_{C_G(v)}(V)$ *has a summand which is a faithful permutation module.*

Proof. Let $F = GF(p)$, $k = \operatorname{End}_{FG}(V)$. Let U be an irreducible summand of $V \otimes_F k$. Then U is a faithful, absolutely irreducible, kG-module, so by Theorem 12 there is a vector $u \in U$ such that $\operatorname{Res}^G_{C_G(u)}(U)$ has a faithful permutation module as a summand. By Lemma 10 there is a vector $v \in V$ with $C_G(v) = C_G(u)$, so the result follows Lemma 9.

Remark. Similarly, the analogue of Theorem 1 of the introduction is valid for all primes p which satisfy Hypothesis 1 of Section 3.

5. CONSEQUENCES FOR GENERAL BLOCKS AND RELATIONSHIPS TO OTHER CONJECTURES

We recall two long-standing conjectures in modular representation theory.

The Alperin-McKay Conjecture. Let B be a p-block with defect group D of a finite group G, and let b be the Brauer correspondent of B for $N_G(D)$. Then $k_0(B) = k_0(b)$. (Recall that $k_0(B)$ is the number of complex irreducible characters in B whose degrees are not divisible by $p[G:D]_p$.)

Brauer's Height Zero Conjecture. Let B be a p-block with defect group D of a finite group G. Then $k_0(B) = k(B)$ if and only if D is Abelian.

The Alperin–McKay conjecture and one-half of Brauer's height zero conjecture are known to have the following consequence, which would also be a consequence of Alperin's weight conjecture, or of conjectures of Broué on the structure of blocks with Abelian defect groups. We state the consequence as another conjecture which would be implied by those above.

Conjecture. Let B be a p-block with Abelian defect group D of a finite group G and let b be the Brauer correspondent of b for $N_G(D)$. Then $k(B) = k(b)$.

Olsson [10] has recently proposed:

Conjecture. Let B be a p-block with defect group D of a finite group G. Then $k_0(B) \leq [D : D']$.

Külshammer proved in [7] (relying ultimately on results of Reynolds [11]) that Olsson's conjecture would be a consequence of the Alperin–McKay conjecture, together with a solution of the $k(GV)$-problem.

We may (using [11] again for part (ii)) state:

THEOREM 13. *Let B be a p-block with defect group D of a finite group G, and let b be the Brauer correspondent for B of $N_G(D)$. Suppose that p satisfies Hypothesis* 1 *of Section* 3 (*in particular, this will hold if $p > 5^{30}$*). *Then*:

(i) *If $k_0(B) = k_0(b)$, we have $k_0(B) \leq [D : D']$.*

(ii) *If D is Abelian and $k(B) = k(b)$, then $k(B) \leq |D|$.*

Proof. (i) Follows from the hypotheses and our Theorem 1, using Külshammer's arguments in [7].

(ii) Follows from the hypotheses, our Theorem 1, and the results of Reynolds [11] which show that there is a block $\tilde{b}$ of a p-solvable group H such that $k(\tilde{b}) = k(b)$ and $\tilde{b}$ has defect group isomorphic to D.

REFERENCES

1. P. Fong, On the characters of p-solvable groups, *Trans. Amer. Math. Soc.* **98** (1961), 263–284.
2. D. Gluck, On the $k(GV)$-problem, *J. Algebra* **89** (1984), 46–55.
3. R. Gow, On the number of characters in a block and the $k(GV)$-problem for self-dual V, *J. London Math. Soc.* (2) **48** (199), 441–451.
4. J. Hall, M. Liebeck, and G. Seitz, Generators for finite simple groups, with applications to linear groups, *Quart. J. Math. Oxford* (2) **43** (1992), 441–458.
5. R. Knörr, On the number of characters in a block of p-solvable group, *Illinois J. Math.* **28** (1984), 181–210.

6. R. Knörr, On Brauer's $k(B)$-conjecture, *J. Algebra* **131** (1990), 444–450.
7. B. Külshammer, A remark on conjectures in modular representation theory, *Arch. Math.* (*Basel*) **49** (1987), 366–369.
8. M. Liebeck, Regular orbits of Linear Groups, *J. Algebra* **184** (1996), 1136–1142.
9. H. Nagao, On a conjecture of Brauer for p-solvable groups, *J. Math. Osaka City Univ.* **13** (1962), 35–38.
10. J. B. Olsson, On the number of characters in blocks, *Math. Z.* **186** (1984), 41–47.
11. W. F. Reynolds, Blocks and normal subgroups of finite groups, *Nagoya Math. J.* **22** (1963), 15–32.
12. G. R. Robinson, Some remarks on the $k(GV)$-problem, *J. Algebra* **172** (1995), 159–166.